

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1-8. (Cancelled)

9. (Currently Amended) In a client computing system, a method for participating in authentication with a server computing system, the method comprising:

an act of the client computing system receiving a first server request that includes at least a first indication of the authentication mechanisms deployed at the server computing system and a server nonce;

an act of the client computing system sending a first response to the server computing system and that includes a client public key, a client nonce and a selected set of at least a second indication of the authentication mechanisms that were included in the first indication of the authentication mechanisms received from the server computing system and that are also deployed at ~~[[both]]~~ the client computing system ~~and the authentication mechanisms deployed at the server computing system~~;

an act of identifying a tunnel key that can be used to encrypt content transferred between the client computing system and the server computing system, the tunnel key comprising a hash of a concatenation of the client public key together with the server nonce and the client nonce;

an act of receiving a second server request that includes encrypted authentication content, the encrypted authentication content being encrypted with the tunnel key and including a server challenge, a mutually deployed authentication method and a trust anchor;

an act of decrypting the encrypted authentication content with the tunnel key to reveal unencrypted authentication content, the unencrypted authentication content ~~indicating a~~ including the mutually deployed authentication mechanism the server challenge and the trust anchor; and

an act of sending a second response to the second server request, the second response including encrypted response data that is responsive to the unencrypted

authentication content, including at least one of a client challenge, a hashed message authentication code that corresponds to the server challenge, or a client authentication signature, the encrypted response data being used for authenticating the client computing system with the server computing system according to the mutually deployed authentication mechanism.

10. (Currently Amended) The method as recited in claim 9, wherein the first server request includes ~~the authentication mechanisms deployed at the server computing system, a~~ previous packet ID corresponding to a previous session existing between the client and the server computing systems and a Nonce.

11. (Original) The method as recited in claim 9, wherein the authentication mechanisms deployed at the server computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

12. (Original) The method as recited in claim 9, wherein the authentication mechanisms deployed at the client computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

13. (Currently Amended) The method as recited in claim 9, wherein the first response includes ~~the authentication mechanisms deployed at the client computing system, a previous packet ID, a nonce, one or more security associations, and one or more~~ a plurality of public keys.

14. (Cancelled).

15. (Currently Amended) The method as recited in claim 9, wherein the act of receiving the second server request comprises receiving encrypted authentication content corresponding to an authentication method selected from among: ~~negotiating an authentication method, re-authenticating,~~ boot-strapping a client with an existing user-name and password, boot-strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

16. (Currently Amended) The method as recited in ~~claim 9~~claim 15, wherein the second server request includes ~~encrypted authentication content, a previous packet ID, a security association, and a public key.~~

17. (Currently Amended) The method as recited in ~~claim 9~~claim 15, wherein the act of sending the second response includes sending encrypted responsive data for an authentication method selected from among: ~~negotiating an authentication method, re-authenticating,~~ boot-strapping a client with an existing user-name and password, boot strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

18. (Currently Amended) The method as recite in ~~claim 9~~claim 16, wherein the second response includes ~~encrypted responsive data and a~~the previous packet ID.

19. (Currently Amended) In a server computing system, a method for participating in authentication with a client computing system, the method comprising:

an act of the server computing system sending a first request that includes at least a first indication of the authentication mechanisms deployed at the server computing system and a server nonce;

an act of the server computing system receiving a first client response to the first request and that includes a client public key, a client nonce and a selected set of at least a second indication of the authentication mechanisms that were included in the first indication of the authentication mechanisms deployed by the server and that are also deployed at ~~both the client computing system, and the authentication mechanisms deployed at the server computing system, the authentication mechanisms deployed at the server computing system being indicated by the first indication;~~

an act of identifying a tunnel key that can be used to encrypt content transferred between the client computing system and the server computing system, the tunnel key comprising a hash of a concatenation of the client public key together with the server nonce and the client nonce;

an act of sending a second request that includes encrypted authentication content, the encrypted authentication content being encrypted with the tunnel key, the encrypted authentication content including a server challenge, indicating a mutually deployed authentication mechanism and a trust anchor; and

an act of receiving a second client response, the second client response including encrypted response data that is responsive to the encrypted authentication content and that includes at least one of a client challenge, a hashed message authentication code corresponding to the server challenge, or a client authentication signature, the encrypted response data being used for authenticating the client computing system with the server computing system according to the mutually deployed authentication mechanism.

20. (Currently Amended) The method as recited in claim 19, wherein the first request includes ~~the authentication mechanisms deployed at the server computing system, a previous packet ID corresponding to a previous session existing between the client and the server computing system and a Nonce.~~

21. (Original) The method as recited in claim 19, wherein the authentication mechanisms deployed at the server computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

22. (Original) The method as recited in claim 9, wherein the authentication mechanisms deployed at the client computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

23. (Currently Amended) The method as recited in claim 19, wherein the first client response includes ~~the authentication mechanisms deployed at the client computing system, a previous packet ID, a nonce, one or more security associations, and one or more~~a plurality of public keys.

24. (Cancelled).

25. (Currently Amended) The method as recited in claim 19, wherein the act of sending a second request comprises sending encrypted authentication content corresponding to an authentication method selected from among: ~~negotiating an authentication method, re-authenticating,~~ boot-strapping a client with an existing user-name and password, boot-strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

26. (Currently Amended) The method as recited in ~~claim 19~~claim 25, wherein the second request includes ~~encrypted authentication content, a previous packet ID, a security association, and a public key.~~

27. (Currently Amended) The method as recited in ~~claim 19~~claim 25, wherein the act of receiving a second client response includes receiving encrypted responsive data for an authentication method selected from among: ~~negotiating an authentication method, re-authenticating,~~ boot-strapping a client with an existing user-name and password, boot strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

28. (Currently Amended) The method as recited in ~~claim 19~~claim 27, wherein the second client response includes ~~encrypted responsive data and a~~the previous packet ID.

29. (New) The method recited in claim 9, wherein the first response also includes a plurality of security associations and wherein the second request includes one of the plurality of security associations selected from the plurality of security associations.

30. (New) The method recited in claim 9, wherein the second response includes the client challenge.

31. (New) The method recited in claim 9, wherein the second response includes the hashed message authentication code.

32. (New) The method recited in claim 9, wherein the second response includes the client authentication signature.